					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P36					Dokumentum címe: **Közösségi média és külső kommunikációs szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. pont	Meghatározott folyamatok és szerepköralapú irányítás a nyilvános kommunikáció kezelésére, biztosítva a pontosságot, a jóváhagyási munkafolyamatokat és az incidensek eszkalációját.
ISO/IEC 27002:2022	5.10, 5.11, 5.35, 5.36 kontrollok	Szabályozza a használatot, az elfogadható használatot, valamint a külső kapcsolattartást, a hatóságokkal folytatott kommunikációt és a megfelelőségi jelentéstételt.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Szabályokat határoz meg a rendszer- és kommunikációhasználatra, a felhasználói értesítésekre és az auditnapló-bejegyzések megőrzésére.
GDPR	5., 25., 32., 33. cikk	Az adatkezelés alapelvei, a beépített és alapértelmezett adatvédelem, az adatkezelés biztonsága, valamint az incidensbejelentési kötelezettségek.
NIS2 irányelv	21. cikk	Kiberbiztonsági kockázatkezelési intézkedések, valamint az incidensekkel és a kockázatokkal kapcsolatos nyilvános kommunikációra vonatkozó kötelezettségek.
DORA-rendelet	9., 16. cikk	IKT-kockázatkezelés és kommunikációs stratégia a kritikus szolgáltatók számára.
COBIT 2019	APO09, DSS05	Szolgáltatási megállapodásokhoz és kommunikációhoz kapcsolódó irányítás, valamint biztonságos kommunikációs gyakorlatok és incidenskezelés.

1. cél

1.1 Jelen szabályzat kötelező érvényű szabályokat és felelősségi köröket határoz meg a szervezettel kapcsolatban álló személyek közösségimédia-használatára és a külső kommunikáció valamennyi formájára vonatkozóan.

1.2 Biztosítja, hogy a nyilvános kommunikáció – legyen az tervezett vagy spontán – pontos, tisztelettel teljes, biztonságos, jogszerű és a vállalati arculattal összhangban álló legyen.

1.3 A szabályzat célja a reputációs kár, a szabályozói nemmegfelelés, a szellemi tulajdon kiszivárgása és a nyilvánosan elérhető csatornákon keresztül történő jogosulatlan közzététel kockázatának minimalizálása.

1.4 A szabályzat továbbá elősegíti az elszámoltathatóságot és a strukturált irányítást a szervezetet érintő vagy arra hatással lévő digitális kommunikáció minden formájában.

2. hatály

2.1 Jelen szabályzat az alábbi személyekre terjed ki: valamennyi munkavállalóra, vállalkozóra, gyakornokra és harmadik fél képviselőjére, akik:

2.1.1 a szervezet nevében kommunikálnak, hivatalos vagy informális formában,

2.1.2 nyilvános környezetben a szervezettel való kapcsolatukra hivatkoznak vagy azt sugallják,

2.1.3 személyes vagy vállalati fiókokat használnak a szervezetet érintő nyilvános kommunikációhoz.

2.2 Az érintett kommunikációs csatornák különösen az alábbiak, de nem kizárólagosan:

2.2.1 közösségimédia-platformok (pl. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook),

2.2.2 blogok, wikik, fórumok és nyilvános üzenőfalak,

2.2.3 e-mail vagy közvetlen üzenetküldés külső felek részére (pl. ügyfelek, szabályozó hatóságok, média),

2.2.4 sajtóinterjúk, panelbeszélgetések vagy rögzített médiaszereplések,

2.2.5 részvétel olyan online közösségekben, ahol a szervezetre hivatkoznak.

2.3 Jelen szabályzat a valós idejű és az előre ütemezett tartalmakra egyaránt vonatkozik, és alkalmazandó minden olyan eszközre és fiókra (személyes vagy vállalati), amelyet a kommunikáció közzétételére használnak.

3. célkitűzések

3.1 Megelőzni a bizalmas, érzékeny vagy szabályozott adatok véletlen vagy szándékos közzétételét külső kommunikációs csatornákon keresztül.

3.2 Biztosítani, hogy a hivatalos nyilvános nyilatkozatok és közösségimédia-tartalmak pontosak, jóváhagyottak és összhangban álljanak a vállalati arculattal, az etikai elvekkel és a stratégiai üzenetekkel.

3.3 Megelőzni a reputációs kárt, és biztosítani az üzenetek következetességét a belső szervezeti egységek és a külső platformok között.

3.4 Megfelelni a nyilvános nyilatkozatokra vonatkozó jogi kötelezettségeknek, ideértve különösen a GDPR, a NIS2, a DORA és az ágazatspecifikus kommunikációs szabályok követelményeit.

3.5 Egyértelmű felelősségi köröket, engedélyezett felhasználási eseteket és érvényesítési eljárásokat meghatározni minden olyan személy számára, aki nyilvánosan elérhető kommunikációs tevékenységet végez.

4. szerepkörök és felelősségek

4.1 Marketing- vagy kommunikációs vezető / PR-felelős

4.1.1 Jóváhagyja a vállalat minden hivatalos, külső közzétételre szánt kommunikációját.

4.1.2 Fenntartja a közösségimédia-tartalomütemezéseket és az arculati következetességet biztosító iránymutatásokat.

4.1.3 Nyomon követi a szervezetet érintő online említéseket és médiaszerepléseket.

4.2 Információbiztonsági vezető / információbiztonsági csapat

4.2.1 Figyelemmel kíséri a digitális platformokat az adatkiszivárgásra, megszemélyesítésre vagy adathalászati kísérletekre utaló jelek szempontjából.

4.2.2 Összehangolja a tevékenységet az incidenskezelő csapatokkal közösségimédia-alapú támadások vagy incidensek esetén.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. betartatás és megfelelés

9.1 Jelen szabályzat az érintett valamennyi munkatársra és harmadik félre nézve kötelező. A nemmegfelelés következménye lehet:

9.1.1 formális figyelmeztetés,

9.1.2 a platformokhoz vagy rendszerekhez való hozzáférés ideiglenes vagy végleges visszavonása,

9.1.3 fegyelmi intézkedések, ideértve a munkaviszony megszüntetését,

9.1.4 jogi eljárás, ha a külső kommunikáció reputációs kárt, adatsértést vagy szabályozói nemmegfelelést eredményez.

9.2 Fegyelmi intézkedések

9.2.1 A belső szabálysértések (pl. bizalmas adatok kiszivárogtatása, a szervezet jó hírnevének megsértése) HR-bevonást, formális vizsgálatot és a munkavállalói nyilvántartásban történő dokumentálást vonnak maguk után.

9.2.2 Amennyiben indokolt, a jogi terület polgári jogi igényeket érvényesít, vagy büntetőjogi cselekmény gyanúja esetén értesíti a hatóságokat (pl. megszemélyesítés, bennfentes kereskedelemhez kapcsolódó kiszivárogtatás).

9.3 A megfelelés nyomon követése

9.3.1 Az információbiztonsági és kommunikációs csapatoknak folyamatos nyomon követést kell végezniük az alábbiak tekintetében:

9.3.1.1 a márkaemlítések a főbb platformokon,

9.3.1.2 a vállalati arculati elemek vagy védjegyek nem hivatalos használata,

9.3.1.3 ismert kockázatok (pl. elégedetlen munkavállalók, megszemélyesítési kísérletek).

9.3.2 A nyomon követést a munkavállalói adatvédelmi jogszabályoknak megfelelően kell végezni, és minden jelzett esetet emberi felülvizsgálónak kell megerősítenie.

9.4 Visszaélés-bejelentés és visszaélésszerű használat jelentése

9.4.1 Minden olyan munkavállalót, aki jelen szabályzat megsértését feltételezi, ösztönözni kell arra, hogy ezt jelentse az információbiztonsági csapatnak, a jogi területnek vagy anonim módon a visszaélés-bejelentő portálon keresztül.

9.4.2 A bejelentőkkel szembeni megtorlás szigorúan tilos, és azonnali fegyelmi intézkedést von maga után.

10. felülvizsgálati és frissítési követelmények

10.1 Jelen szabályzatot évente, vagy ennél korábban felül kell vizsgálni, ha:

10.1.1 jelentős változás következik be a szabályozói követelményekben (pl. új uniós digitális kommunikációs jogszabályok),

10.1.2 új közösségimédia-platformok vagy kommunikációs csatornák kerülnek bevezetésre,

10.1.3 jelentős incidens vagy ismétlődő szabálysértések arra utalnak, hogy folyamathiányosság áll fenn,

10.1.4 strukturális vagy vezetői változás történik a PR-, jogi vagy információbiztonsági területen.

10.2 A felülvizsgálatot közösen az alábbiak végzik:

10.2.1 a marketing-/PR-vezető,

10.2.2 az információbiztonsági vezető vagy a biztonsági kockázatokért felelős vezető,

10.2.3 a jogi és megfelelőségi vezetők.

10.3 A frissítéseket a szabályzatváltozási nyilvántartásban dokumentálni kell, és belső tudatossági csatornákon kommunikálni kell. Lényeges változások esetén minden érintett munkatársnak ismételten meg kell erősítenie a szabályzat tudomásulvételét.

11. kapcsolódó szabályzatok és összefüggések

11.1 Jelen szabályzatot a szervezet információbiztonság-irányítási rendszerének (ISMS) alábbi elemei támogatják, és azokkal szoros összefüggésben értelmezendő:

11.1.1 P1 – Információbiztonsági szabályzat: meghatározza az információk védelmének átfogó alapelveit, ideértve annak biztosítását is, hogy a kommunikáció ne vezessen jogosulatlan közzétételhez.

11.1.2 P3 – Elfogadható használati szabályzat: meghatározza a digitális platformok és technológiák elfogadható használatát, amely közvetlenül irányadó a közösségi csatornák személyes és szakmai használatára.

11.1.3 P6 – Kockázatkezelési szabályzat: meghatározza a nyilvános kommunikációval és a reputációs kitettséggel kapcsolatos fenyegetések értékelésére szolgáló kockázatkezelési keretrendszert.

11.1.4 P8 – Információbiztonsági tudatossági és képzési szabályzat: előírja azokat a tudatosságnövelő programokat, amelyek a munkatársakat a biztonságos kommunikációs gyakorlatokról és a szociális manipulációs fenyegetésekről oktatják.

11.1.5 P13 – Adatosztályozási és címkézési szabályzat: iránymutatást ad arra vonatkozóan, mi minősül korlátozott vagy bizalmas információnak, amely külső fél részére nem hozható nyilvánosságra.

11.1.6 P30 – Incidenskezelési szabályzat: meghatározza a nyilvános kommunikációval összefüggő incidensek kezelésének módját, ideértve az adatszivárgást, a megszemélyesítést és a szabályozói nemmegfelelést.

11.1.7 P33 – Audit- és megfelelőségfelügyeleti szabályzat: szabályozza azokat az auditfolyamatokat, amelyek ellenőrzik a közösségimédia-kontrollokat, a megfigyelési rendszereket és a külső kommunikációs szabályzatoknak való megfelelést.

12. hivatkozott szabványok és keretrendszerek

12.1 ISO/IEC 27001:

12.1.1 8.1 pont – Működéstervezés és -szabályozás: előírja a meghatározott folyamatokat és a szerepköralapú irányítást a nyilvános kommunikáció kezelésére, biztosítva a pontosságot, a jóváhagyási munkafolyamatokat, valamint az adatokkal vagy reputációs kockázattal összefüggő incidensek eszkalációját.

12.2 ISO/IEC 27002:2022:

12.2.1 5.10 kontroll – Információk használata: szabályozza a belső vagy külső kommunikáció engedélyezett és etikus közzétételét.

12.2.2 5.11 kontroll – Az információk és eszközök elfogadható használata: megerősíti a vállalati eszközökkel vagy személyes fiókokkal történő tartalommegosztás elfogadható gyakorlatát.

12.2.3 5.35 kontroll – Kapcsolattartás a hatóságokkal: előírja a strukturált és felhatalmazott külső kommunikációt a szabályozó hatóságokkal és közintézményekkel.

12.2.4 5.36 kontroll – Megfelelés a szabályzatoknak és szabványoknak: előírja a belső szabályzatok következetes alkalmazását minden kommunikációs helyzetben.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Magatartási szabályok: előírja a rendszer- és kommunikációhasználatra vonatkozó formális szabályokat, ideértve a nyilvános közzététel szabályait is.

12.3.2 AC-8 – Rendszerhasználati értesítés: támogatja a kötelező nyilatkozatok és tartalmi figyelmeztetések alkalmazását a külső felületeken.

12.3.3 AU-12 – Auditnapló-bejegyzések megőrzése: alkalmazandó a naplók és a kommunikációs előzmények megőrzésére incidensfelülvizsgálati és auditcélokból.

12.4 GDPR (2016/679):

12.4.1 5. cikk – Az adatkezelés alapelvei: tiltja a személyes adatok jogosulatlan megosztását nyilvános kommunikáció útján.

12.4.2 25. cikk – Beépített és alapértelmezett adatvédelem: előírja az adatvédelmi biztosítékokat a kommunikációs eszközökben és a tartalomkezelési munkafolyamatokban.

12.4.3 32. cikk – Az adatkezelés biztonsága: alkalmazandó a titkosításra, a hozzáférés-szabályozásra és a tartalomjóváhagyási folyamatokra.

12.4.4 33. cikk – Incidensbejelentés: előírja a személyes adatok nyilvános csatornákon keresztüli kiszivárgásának időben történő bejelentését.

12.5 NIS2 irányelv (2022/2555):

12.5.1 21. cikk – Kiberbiztonsági kockázatkezelési intézkedések: magában foglalja a kommunikációs protokollokat és az incidensekhez, valamint a kockázatokhoz kapcsolódó nyilvános kommunikáció során fennálló kötelezettségeket.

12.6 DORA-rendelet (2022/2554):

12.6.1 9. cikk – IKT-kockázatkezelés: alkalmazandó a kívülről kiváltott kommunikációs kockázatokra, mint a megszemélyesítés, a félretájékoztatás és a reputáció megzavarása.

12.6.2 16. cikk – Kommunikációs stratégia: előírja, hogy a kritikus pénzügyi vagy szolgáltató szervezetek válsághelyzetben kezeljék a kommunikációs kockázatokat és a kapcsolódó reagálást.

12.7 COBIT 2019:

12.7.1 APO09 – Menedzselt szolgáltatási megállapodások és kommunikáció: előírja a belső és külső kommunikáció strukturált irányítását.

12.7.2 DSS05 – Biztonsági szolgáltatások kezelése: biztosítja, hogy a kommunikációs tevékenységek ne vezessenek többletkockázathoz, és ne gyengítsék az incidenskezelési folyamatokat.